CLAIMS

1. In a wireless network comprising a server and server software including an intelligent software agent, a method of automatically providing a secure connection between the wireless network and a user-operated device seeking access to the wireless network, the method comprising:

in response to an initial request for access to the wireless network by the device -

(a) automatically installing the software agent on the device;

(b) executing the software agent on the device to gather information from the requesting device, including device information and user authentication information;

(c) transmitting the device identification and user authentication information to the server; and

(d) verifying the device identification and user authentication information; wherein when successfully verified, storing the identification and authentication information on an authorized access list, providing a unique encryption key to the device for storage thereon and granting the requesting device access to the wireless network; and when unsuccessfully verified, storing the identification and authentication information on an unauthorized access list and denying the device access to the wireless network.

2. The method of claim 1 further comprising, in response to a subsequent request for access to the wireless network by the device -

(a) receiving the unique key corresponding to the device;

(b) retrieving the identification and authentication information corresponding to the unique key;

(c) comparing the identification and authentication information with the authorized and unauthorized lists; and

(d) based on the comparison, one of granting and denying the device access to the wireless network.

3. The method of claim 1, wherein the step of denying access comprises generating a notification message that an unauthorized device has attempted to access the network.

4. The method of claim 1, wherein the step of granting access comprises providing access in accordance with existing network access rights of the user operating the device.

5. The method of claim 1, further comprising the step of collecting information relevant for billing the user for services accessed through the network.

6. The method of claim 1, further comprising the step of collecting information relevant for bandwidth allocation over the network.

7. The method of claim 1, further comprising the step of determining the geographical location of the device.

8. The method of claim 1, further comprising the step of automatically installing application software on the device.

9. The method of claim 1, wherein the encryption key is a certificate.

10. The method of claim 1, wherein the network comprises an isolated network segment and the initial connection between the device and the network is limited to the isolated network segment.

11. The method of claim 1, wherein the step of granting access further comprises conformity to a security policy with respect to access from multiple devices.

12. The method of claim 1, wherein the user is defined as a guest user and given a temporary encryption key with guest network access rights.